Impact of Management Data Placement in NFV Service Coordinated Across Multiple Datacenters and WANs

Atsushi Taniguchi, Takahiro Yamazaki, Yasuhiro Yoshida, Taichi Kawabata, Norio Sakaida, and Takashi Shimizu
NTT Network Innovation Laboratories
1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa 239-0847 Japan
taniguchi.atsushi@lab.ntt.co.jp

***Abstract*— As network function virtualization (NFV) technologies have emerged, some standardization bodies such as the ETSI have advanced standardization activities on their functional blocks and interfaces. However, several issues such as where virtual network configuration information should be placed or how virtual network configuration among Virtualized Infrastructure Managers (VIMs) should be handled have not been standardized yet. This paper proposes several candidates to address these issues, and discusses their advantages and disadvantages from various viewpoints such as security.**

Keywords*— *Network function virtualization, management and orchestration, wide area network, network controller, multiple datacenters, configuration information, interconnection

I. INTRODUCTION

Recently, advancements in virtualization technologies have enabled venders and service providers to provide flexible and highly-available cloud services [1][2]. In order to provide a long-term and interoperable operating environment, the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) for Network Function Virtualization (NFV) and the Open Networking Foundation standardized an architecture for NFV and Software Defined Networking (SDN) [1][2].

Virtual Network Integration as a Service (VNIaaS) was proposed recently in [3] and enables service providers that do not have their own network and cloud resources to provide NFV services using leased virtual networks and cloud resources from multiple infrastructure providers. In such a case, the placement of the management data is important in terms of security, since one infrastructure manager cannot access the non-disclosed configuration information of another manager. Therefore, when a Network Service (NS) is coordinated across multiple datacenters through a Virtual Private Network (VPN), we need to configure the IP address of the network elements manually.

In this paper, we evaluate the advantages and disadvantages of several candidate locations for placement of the configuration information from the aspects of performance, operation, management, and security. We also propose a mechanism to exchange configuration parameters among datacenters and WANs.

978-3-901882-77-7 (c) 2015 IFIP

II. PREVIOUS WORK

The ETSI defines network function blocks to manage Virtualization Network Functions (VNFs) as a NFV reference architectural framework [4]. Fig. 1 shows the NFV reference architectural framework defined by the ETSI ISG NFV standard.

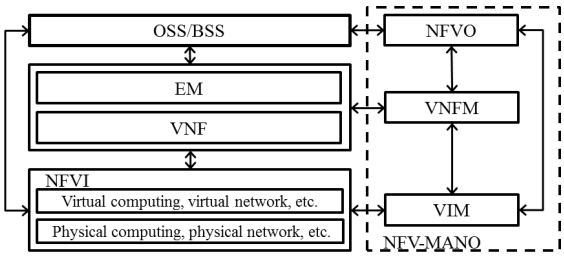

Fig. 1. NFV reference architectural framework.

The NFV reference architectural framework is divided into four function blocks: the VNF, NFV Infrastructure (NFVI), NFV Management and Orchestration (NFV-MANO), and Operation Support System/ Business Support System (OSS/BSS). A VNF is the virtualization of a network function in a legacy non-virtualized network, the NFVI is the hardware and software components that comprise the environment in which the VNFs are deployed, the NFV-MANO manages all of the NFV platforms, and the OSS/BSS manages the legacy network. NFV-MANO is divided into the VNF Manager (VNFM), Virtualized Infrastructure Manager (VIM), WAN Infrastructure Manager (WIM), and NFV Orchestrator (NFVO). The VNFM manages the VNF instance, and the VIM and WIM manage the allocation of the NFVI. The NFVO manages the NSs that are provided by the NFV and the NFVI resources across multiple VIMs.

If the NFVO allocates the WAN resource, the NFV environment is divided into two cases: the first is where the network infrastructure is provided by a single operator, and the second is where the network infrastructure is provided by multiple operators. Fig. 2 shows an example of the network environment for NS deployment through multiple-managed domains provided by a single operator.

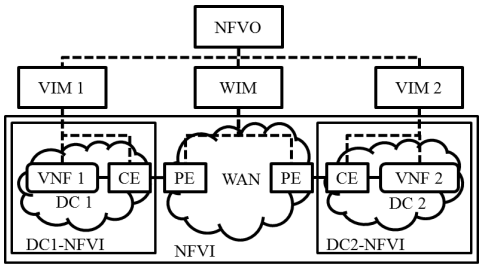

Fig. 2. NFV architecture provided by single operator.

VIM 1 and VIM 2 control the NFVI of Data Center (DC) 1, DC 2, respectively and provide network connectivity between the VNF and Customer Edge node (CE), and the WIM provides network connectivity between the CE of DC 1 and DC 2. Therefore, the VNFs of DC 1 and DC 2 can connect to each other through a WAN.

Fig. 3 shows an example of a NS deployment through multiple managed domains provided by multiple operators. The VIM/WIM and NFVI are provided by the infrastructure providers and the NFVO is provided by the service provider. The NFVO controls the network resources through the application programming interface of the VIM or WIM.

III. ISSUES

A. Placement of Management Data

In the case of a NFV service among multiple managed domains through a WAN as in Fig. 3, the NFVO has difficulty in sorting and selecting the required information because the configuration information is located in geographically separated domains that are managed by multiple infrastructure providers. Although the ETSI has standardized a number of function blocks and the interface between blocks, if the placement of the configuration information is underspecified, the interface of the blocks would not be decided.

Thus, we address various issues and the placement of the configuration information from the aspects of performance, operation, management, and security in Section IV.

B. Exchanging Configuration Information among Operators

Usually, network operators use the Border Gateway Protocol (BGP) to establish an inter-domain connection. The BGP can exchange routing information through multiple managed domains by exchanging network layer reachability information dynamically. It is possible to achieve effective operation by managing the policies of the BGP dynamically. However, configuration of the BGP is independently performed in each domain and information regarding the configurations cannot be exchanged with other domains.

Thus, hereafter we address various issues and the means for exchanging the configuration information among multiple managed domains from the aspects of performance, operation, management, and security in Section V.

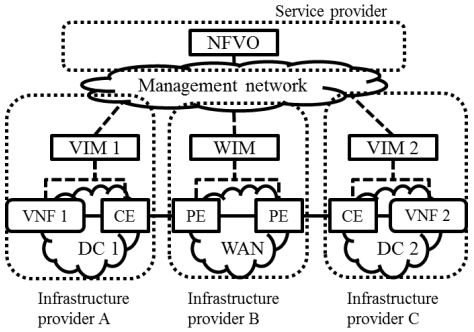

Fig. 3. NFV architecture provided by multiple operators.

IV. PLACEMENT OF CONFIGURATION INFORMATION

There are two cases for the location of the management database (DB): the first is on the NFVO side (NFVO case) and the other is on the VIM/WIM side (VIM case). We evaluate the advantages and disadvantages with respect to these two cases.

A. Query Response Time

In the case of a NFV service through a WAN, function blocks of the NFVO, VIM, and WIM are located in geographically separated areas.

The queuing time and latency due to the inquiry from the NFVO until the response from the VIM and WIM affect the response time in a direct fashion. In order to compare models simply, we consider the case of a simple query of the NS configuration information from the OSS/BSS. For the NFVO case, the NFVO searches database its own database and replies to the OSS/BSS. Thus, the NFVO case is modeled as a queuing model *M/M/1*. On the other hand, for the VIM case, the NFVO queries the NS information to the VIM/WIM which has the database of NS information after request of the OSS/BSS. The VIM searches own database and reply to the NFVO. Then the NFVO forwards the configuration information to the OSS/BSS. Therefore the VIM case is modeled as a queuing model for *M/M/m*. The number of VIMs and WIMs are represented as "*m*" and the volumes of configuration information for the VIM and WIM are approximately the same.

Fig. 4 shows a model that explains the placement of the management DB. In the NFVO case, the query response time, T_{nfvo}, is given as (1), where λ and $1/\mu_{nfvo}$ represent the query rate of users and the processing time of the NFVO, respectively.

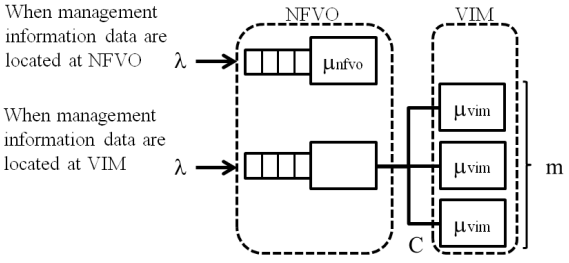

Fig. 4. Modeling according to placement of management DB.

$$T_{nfvo}=1/(\mu_{nfvo}-\lambda) \quad (1)$$

In the VIM case, the query response time T_{vim} is given as (2) where λ, P_m, $1/\mu_{vim}$, and C represent the query rate of users, probability of waiting state for the VIMs, the processing time of the NFVO, and a constant parameter for the round time delay among the NFVO and VIMs, respectively.

$$T_{vim}=1/\mu_{vim}+P_m/(m\mu_{vim}-\lambda)+C \quad (2)$$

Fig. 5 shows the calculated results (C = 20 ms, m = 3, $1/\mu_{nfvo}$= 30 ms, $1/\mu_{vim}$= 30 ms) . If the query rate is lower, T_{nfvo} will be shorter than T_{vim} because $P_m \cong 0$. As results, the NFVO case is better response. On the other hand, If the query rate is higher, T_{vim} will be shorter than T_{nfvo} because $P_m \cong 1$ and $\lambda/\mu \cong 1$. As results, the VIM case is better response.

B. Scalability

When creating a NS, in the NFVO case, the NFVO searches the VIMs that can fulfill the policy and resource requirements from the OSS/BSS. Then the NFVO queries the selected VIMs and WIMs to create the NS and the NFVO must register the configuration information in the management DB after creating the NS at the VIMs and WIMs. If some VIMs and WIMs are used at the same time, then the writing operation of the management DB is concentrated especially at a higher queue rate.

On the other hand, in the VIM case, the reading and writing operation of the management DB and that for the NS creation are performed at each VIM and WIM. Therefore, the load on the NFVO is lower and the management database operations have a low impact on the entire service.

C. Operation and Management

In the NFVO case, the management DB is only located in the NFVO. If a failure occurs in the NFVO, management DB, or control plane (C-plane), the VIM and WIM cannot access the management DB.

As a result, if a failure occurs, all service information would become unavailable. In the VIM case, even if a failure occurs, the VIM can recover from the failure locally, and the failure does not influence the service of other VIMs.

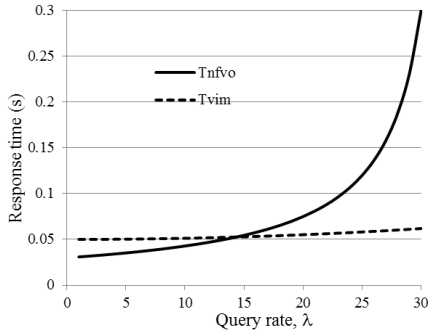

Fig. 5. Calculation results.

D. Security

In terms of the user management, the NFVO case can easily control the identification [5]. However in terms of the configuration information, the operator of the infrastructure provider is quite unlikely to access the configuration information of another operator. Thus, for the case with multiple operators, only the VIM case is selected.

E. Migration

The management DB is managed by the OSS/BSS in the non-virtualized conventional case. In such a case, migrating the management DB is easier in the NFVO case because the NFVOs are the same as those for the OSS/BSS. On the other hand, a step-by-step migration plan is required for the VIM case because the VIMs are located in geographically separated areas.

Table I shows comparison results relevant to the placement of the management DB. If the service volume is small and the service is completed using a single operator, the NFVO case is suitable. However, if the service volume is large or the service infrastructure is provided by multiple operators, the VIM case is more suitable.

TABLE I. COMPARISON RESULTS RELEVANT TO PLACEMENT OF MANAGEMENT DB

	NFVO Side	VIM/WIM Side
Response time for query	Short with low query rate, Long with high query rate	Short regardless of query rate
Scalability	Concentrate load of NFVO	Independent of NFVO
Operation and management	Failure impacts entire service	Possible to recover from failure inside VIM domain
Security	Only for single operator	For multiple operators
Migration	Easy	Step-by-step migration plan is required
Application	Low query rate, single operator	High query rate, multiple operators

V. EXCHANGING CONFIGURATION INFORMATION

As described in Section III, exchanging configuration information among the VIMs and WIMs can achieve efficient operation. However, there is no official interface for exchanging configuration information among VIMs and WIMs in the ETSI ISG NFV standard [4]. Therefore, an alternative way to exchange the required information for the edge nodes is conceived. In this section, we compare three routes to exchange messages in Fig. 6 as given hereafter.

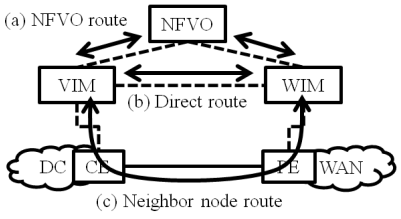

Fig. 6. Exchange route for configuration information for VIM and WIM.(a) NFVO route: a route through the NFVO (b) Direct route: a route that directly connects the VIM and WIM (c) Neighbor node route: a route through a link between the edge nodes

A. Scalability

For a *NFVO route*, the NFVO receives a message from one VIM/WIM and forwards the message to its counterpart VIM/WIM. If the NFVO receives many queries, the load on the NFVO is concentrated. On the other hand, for a *direct route*, the communications between the VIM and WIM are independent of the load on the NFVO. For the case of a *neighbor node route*, because the exchange route of the configuration information overlaps the user traffic in the data plane (D-plane), traffic management such as the Quality of Service (QoS) is required to prevent packet loss of the user data.

B. Operation and Management

Even if something fails in the C-plane, we can see that there is no effect as in Figs. 6(a), (b), and (c). However, for the case of a *neighbor node route*, if the connection between the neighbor nodes is down, the VIM cannot access its counterpart VIM through the neighbor node route. In such a case, the NFVO must access the VIM or WIM and recover the connection between the neighbor nodes of the VIM and WIM.

C. Security

In the case of a *NFVO route,* the NFVO exchanges the configuration information through the *NFVO route*. Because the configuration information is private information of the infrastructure provider, the NFVO requires technology to prevent the leakage of information and mutual authentication among the NFVO and VIMs. For the case of the *neighbor node route*, the probability that the information will be leaked is low because of the independent communications route. For the case of the *direct node*, it is not realistic to establish a connection among multiple operators because the C-plane must be connected to the VIM and WIM.

Table II shows comparison results related to the exchange routes. If the management DB is located on the NFVO side, the NFVO route is suitable. If the management DB is located on the VIM side and the infrastructure is provided by multiple operators, the NFVO route or the neighbor node route is suitable. If the infrastructure is provided by a single operator, all of routes are available.

TABLE II. COMPARISON RESULTS BASED ON ASPECTS OF EXCHANGE ROUTE

	NFVO Route	Direct Route	Neighbor Node Route
Scalability	Load of NFVO is concentrated	Good	Configuration of QoS is required
Operation and management	Does not affect service	Does not affect service	Does not affect service
Security	Information filtering technologies and authentication technology are required	Control plane connection is required	Multiple operators can use this route by using VPN connection
Application	•NFVO side •single or multiple operators	•VIM side •single operators	•VIM side •single or multiple operators

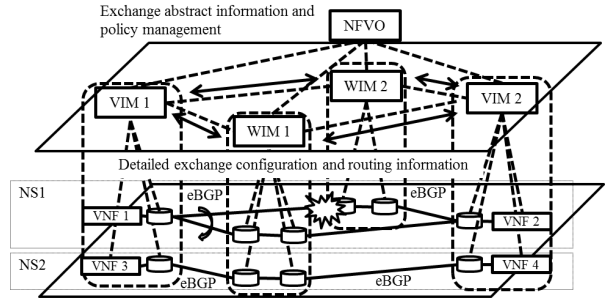

Fig. 7. Proposed NFV system coordinated across multiple datacenters.

VI. PROTOTYPE

We propose a NFV system for exchanging the configuration message among the VIM and WIM domains for the Inter-cloud service use case [6][7]. Fig. 7 shows the proposed NFV system. The OSS/BSS requests NS creation by specifying a NS catalogue. The NFVO provides abstract network and policy information to the VIMs and WIMs in the management plane (M-plane), and the VIMs and WIMs compute the detailed routing information. The NFVO verifies the virtual resources allocated to the VNFM and VIM by specifying the policy information. Then the policy information is used to control the routing policy with respect to each NS such as the acceptable bandwidth and delay. Then the VIM exchanges the configuration information of the edge nodes among the VIMs and WIMs over the C-plane.

VII. SUMMARY

We discussed the placement of the management database and showed the optimal placement with respect to each considered usage case and also discussed exchanging the configuration information through multiple domains and showed the optimal means for the usage cases. The results show that the placement of the management database has an impact on the scalability, operation, and security of the NS.

In the future, we will create a prototype of the proposed architecture and evaluate it from the aspects of management and operation.

REFERENCES

[1] "Network Functions Virtulisation-Introductory White Paper," ETSI, Oct. 2012.

[2] "Software-Defined Networking: The New Norm for Networks," ONF white paper, 2012.

[3] W. Shen, M. Yoshida, K. Minato, and W. Imajuku, "vConductor: An enabler for achieving virtual network integration as a service," IEEE Commun. Mag, vol. 53, no. 2, pp. 116-124, Feb. 2015.

[4] "ETSI GS NFV-MAN 001 v1.1.1" ETSI, 2014.

[5] A. Celesti, F. Tusa, M. Villari, A. Puliafito, "Security And Cloud Computing: Intercloud Identity Management Infrastructure", Proceedings of The 19th IEEE International Workshops on Enabling Technologies, Tei of Larissa, Greece June 2010.

[6] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, M. Morrow, "Blueprint for the Intercloud-Protocols and Formats for Cloud Computing Interoperability," in Internet and Web Applications and Services (ICIW), 2009

[7] M. Mechtri, I. Houidi, W. Louati, D. Zeghlache, "SDN for Inter Cloud Networking," in Future Networks and Services (SDN4FNS), 2013